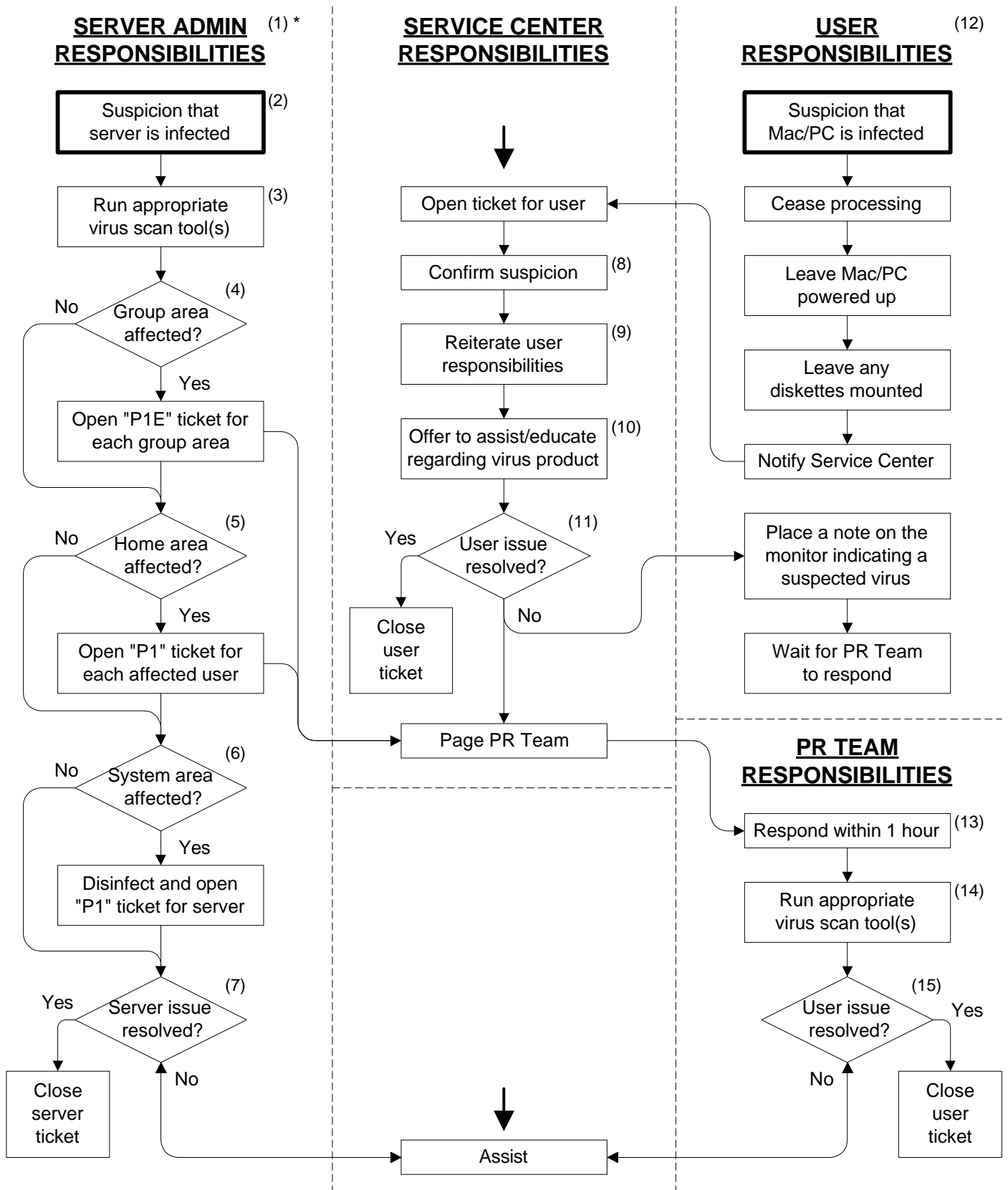# VIRUS RESPONSE PROCESS

(for security incidents, see Incident Response Process)

OBJECTIVE: Achieve high effectiveness and efficiency in virus response, and enlighten all affected parties to enable better virus protection.

SERVER ADMIN RESPONSIBILITIES (1) *

- Suspicion that server is infected (2)
- Run appropriate virus scan tool(s) (3)
- Group area affected? (4) — No / Yes
- Open "P1E" ticket for each group area
- Home area affected? (5) — No / Yes
- Open "P1" ticket for each affected user
- System area affected? (6) — No / Yes
- Disinfect and open "P1" ticket for server
- Server issue resolved? (7) — Yes / No
- Close server ticket

SERVICE CENTER RESPONSIBILITIES

- Open ticket for user
- Confirm suspicion (8)
- Reiterate user responsibilities (9)
- Offer to assist/educate regarding virus product (10)
- User issue resolved? (11) — Yes / No
- Close user ticket
- Page PR Team

USER RESPONSIBILITIES (12)

- Suspicion that Mac/PC is infected
- Cease processing
- Leave Mac/PC powered up
- Leave any diskettes mounted
- Notify Service Center
- Place a note on the monitor indicating a suspected virus
- Wait for PR Team to respond

PR TEAM RESPONSIBILITIES

- Respond within 1 hour (13)
- Run appropriate virus scan tool(s) (14)
- User issue resolved? (15) — No / Yes
- Close user ticket

- Assist

* See notes on back

22-Apr-98